CLAIMS

What is claimed is:

1. A method for establishing a secure context for communicating messages between a first system and a second system, the method comprising:

obtaining by the second system a first public key certificate of the first system, wherein the second system is able to validate the first public key certificate that contains a public key;

generating by the second system a transport key, wherein the transport key is a symmetric secret key;

placing by the second system the transport key and an authentication token into a first message secured with the public key;

sending the first message from the second system to the first system;

receiving at the second system from the first system a second message secured with the transport key in response to sending the first message to the first system;

extracting by the second system a session key from the second message, wherein the session key is a symmetric secret key; and

employing the session key to secure subsequent messages sent by the second system to the first system.

2. The method of claim 1 wherein the authentication token comprises a second public key certificate of the second system, and wherein the first system is able to validate the second public key certificate.

3. The method of claim 2 further comprises:

decrypting, by the second system using a private key associated with the second public key certificate, a digital envelope in the second message containing the session key, wherein the digital envelope was created by the first system using a public key contained in the second public key certificate.

4. The method of claim 1 wherein the authentication token comprises a username-password pair.

5. The method of claim 1 wherein the authentication token comprises a secure ticket.

6. A method for establishing a secure context for communicating messages between a first system and a second system, the method comprising:

providing by the first system a public key certificate associated with the first system, wherein the second system is able to validate the public key certificate;

receiving at the first system from the second system a first message, wherein the first message is secured with a public key from the public key certificate associated with the first system, wherein the first message contains a transport key and an authentication token, and wherein the transport key is a symmetric secret key;

authenticating the second system by the first system based on the authentication token;

generating by the first system a session key, wherein the session key is a symmetric secret key;

placing by the first system the session key into a second message secured with the transport key;

sending the second message from the first system to the second system in response to receiving the first message; and

receiving at the first system from the second system subsequent messages secured with the session key.

7. The method of claim 6 wherein the authentication token comprises a public key certificate associated with the second system.

8. The method of claim 7 further comprising:

creating, by the first system using a public key contained in the public key certificate associated with the second system, a digital envelope in the second message containing the session key.

9. The method of claim 6 wherein the authentication token comprises a username-password pair.

10. The method of claim 6 wherein the authentication token comprises a secure ticket.

11. A computer program product on a computer readable medium for use in a second system for establishing a secure context for communicating messages between a first system and the second system, the computer program product comprising:

means for obtaining a public key certificate containing a public key associated with the first system;

means for generating a transport key, wherein the transport key is a symmetric secret key;

means for placing the transport key and an authentication token into a first message secured with the public key;

means for sending the first message to the first system;

means for receiving from the first system a second message secured with the transport key in response to sending the first message to the first system;

means for extracting a session key from the second message, wherein the session key is a symmetric secret key; and

means for employing the session key to secure subsequent messages sent to the first system.

12. The computer program product of claim 11 wherein the authentication token comprises a second public key certificate associated with the second system, a username-password pair, or a secure ticket.

13. A computer program product on a computer readable medium for use in a first system for establishing a secure context for communicating messages between a first system and the second system, the computer program product comprising:

means for providing a public key certificate associated with the first system;

means for receiving a first message from the second system, wherein the first message is secured with a public key from the public key certificate associated with the first system, wherein the first message contains a transport key and an authentication token, and wherein the transport key is a symmetric secret key;

means for authenticating the second system based on the authentication token;

means for generating a session key, wherein the session key is a symmetric secret key;

means for placing the session key into a second message secured with the transport key;

means for sending the second message to the second system in response to receiving the first message; and

means for receiving from the second system subsequent messages secured with the session key.

14. The computer program product of claim 13 wherein the authentication token comprises a public key certificate associated with the second system, a username-password pair, or a secure ticket.

15. An apparatus for establishing a secure context for communicating messages between a first system and a second system, the apparatus comprising:

means for obtaining a public key certificate containing a public key associated with the first system;

means for generating a transport key, wherein the transport key is a symmetric secret key;

means for placing the transport key and an authentication token into a first message secured with the public key;

means for sending the first message to the first system;

means for receiving from the first system a second message secured with the transport key in response to sending the first message to the first system;

means for extracting a session key from the second message, wherein the session key is a symmetric secret key; and

means for employing the session key to secure subsequent messages sent to the first system.

16. The apparatus of claim 15 wherein the authentication token comprises a second public key certificate associated with the second system, a username-password pair, or a secure ticket.

17. An apparatus for establishing a secure context for communicating messages between a first system and a second system, the apparatus comprising:

means for providing a public key certificate associated with the first system;

means for receiving a first message from the second system, wherein the first message is secured with a public key from the public key certificate associated with the first system, wherein the first message contains a transport key and an authentication token, and wherein the transport key is a symmetric secret key;

means for authenticating the second system based on the authentication token;

means for generating a session key, wherein the session key is a symmetric secret key;

means for placing the session key into a second message secured with the transport key;

means for sending the second message to the second system in response to receiving the first message; and

means for receiving from the second system subsequent messages secured with the session key.

18. The apparatus of claim 17 wherein the authentication token comprises a public key certificate associated with the second system, a username-password pair, or a secure ticket.